Computer Networks 57 (2013) 3098–3111

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

DARE: evaluating Data Accuracy using node REputation

Sabrina Sicari [a,*], Alberto Coen-Porisini [a], Roberto Riggio [b]

[a] Università degli studi dell'Insubria, Dipartimento di Scienze Teoriche e Applicate, Via Mazzini, 5, 21100 Varese, Italy
[b] CREATE-NET, Via Alla Cascata 56/C, 38123 Trento, Italy

ARTICLE INFO

Article history:
Received 2 May 2013
Accepted 11 July 2013
Available online 31 July 2013

Keywords:
Sensors networks
Mesh architecture
Secure aggregation
Localization
Verifiable multilateration
Simulations

ABSTRACT

Typical wireless sensor networks (WSNs) applications are characterized by a certain number of different requirements such as: data accuracy, localization, reputation, security, and confidentiality. Moreover, being often battery powered, WSNs face the challenge of ensuring privacy and security despite power consumption limitations. When the application scenario allows their use, data aggregation techniques can significantly reduce the amount of data exchanged over the wireless link at the price of an increased computational complexity and the potential exposition to data integrity risks in the presence of malicious nodes. In this paper, we propose DARE, an hybrid architecture combining WSNs with the wireless mesh networking paradigm in order to provide secure data aggregation and node reputation in WSNs. Finally, the use of a secure verifiable multilateration technique allows the network to retain the trustworthiness of aggregated data even in the presence of malicious node. Extensive performance evaluations carried out using simulations as well as a real-world prototype implementation, show that DARE can effectively reduce the amount of data exchanged over the wireless medium delivering up to 50% battery lifetime improvement to the wireless sensors.

1. Introduction

In the recent years the number of applications using wireless sensor networks (WSNs) has dramatically increased and therefore requirements such as data accuracy, localization, reputation, security, and confidentiality are becoming more and more important in many application scenarios. Moreover, since WSNs are very often battery powered, optimizing the power consumption of wireless sensors nodes is considered of vital importance by both researchers and practitioners.

Thus, it is necessary to design WSNs meeting the above requirements while satisfying the power constraints imposed by the technology. Notice that such requirements are very often related one another. For instance, in a WSN monitoring physical quantities (e.g., temperature), data accuracy depends on nodes position since it is necessary to know where sensors are located in order to have an accurate picture of the status of the monitored environment. Since the position of sensor nodes is often computed by means of nodes cooperation, attacks such as node displacement; wormholes fabricated communication links; distance enlargement by introducing fake nodes; dissemination of false position and distance information by compromising nodes, may lead to an incorrect information about nodes position, threatening in this way the security of the whole WSN.

Typical security and privacy techniques used in wireless networks are not directly applicable to WSNs due to their needs in terms of power consumption. A possible solution is represented by a technique known as Verifiable Multilateration (VM) [1] that allows one to determine the level of trustworthiness associated with the position reported by a sensor node based on the previous behavior of the node itself. In other words nodes are associated with a level of

* Corresponding author. Tel.: +39 332 218924.
E-mail addresses: sabrina.sicari@uninsubria.it (S. Sicari), alberto.coen-porisini@uninsubria.it (A. Coen-Porisini), roberto.riggio@create-net.org (R. Riggio).

1389-1286/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.comnet.2013.07.014

reputation representing trustworthiness. Therefore, data coming from nodes having a good reputation, are considered trustworthy, while data coming from nodes having a bad reputation are not.

Another way to reduce the overall power consumption of a WSN is based on minimizing the number of data transmissions, since this operation is the most energy demanding one. This can be done by using data aggregation techniques [2,3], which can significantly reduce the amount of data exchanged over the wireless link, while increasing the amount of computation performed by sensor nodes. However, data aggregation raises several privacy and security issues since it is potentially vulnerable to attackers who, for instance, may inject bogus information without being detected. Secure aggregation techniques, such as the one defined by Castelluccia et al. [4], which guarantees end-to-end confidentiality and integrity to the aggregated data, can be used to overcome such issues.

However, data aggregation, verifiable multilateration along with other known techniques may not be enough to ensure the level of security required within the power constraints imposed by the WSN technology. In fact, the limited WSN resources in term of power on one hand and the application requirements on the other hand, call for new solutions. Thus, we decided to move from the traditional architecture comprising only wireless sensor nodes and use a hybrid architecture, that is the combination of two or more network architectures, in order to exploit the capabilities offered by the integration of different technologies.

In this paper, we introduce DARE (evaluating Data Accuracy using node REputation), an hybrid architecture combining WSNs and wireless mesh networks (WMNs) exploiting the gateway/bridge functionalities of mesh routers that allows the integration of WMNs with other networks [5]. Sensor nodes provide only sensing functionalities and they forward sensed data to the closest mesh router. Mesh routers, in turn, provide secure data aggregation and node localization capabilities and are in charge of relaying the aggregated data to the *Sink*. Such an architecture reduces the amount of data exchanged over the network, by splitting the required functionalities between sensor nodes and mesh routers leaving the latter in charge of the more computationally intensive tasks.

We already investigated secure and energy efficient WSNs in some of our previous works [6–11]. More specifically, in [11] we defined a hybrid solution between wireless sensors and mesh networks to perform secure data aggregation without taking into account node localization nor node reputation. DyDAP [6] presented an approach coupling a privacy management policy with an original aggregation algorithm able to deal with end-to-end encrypted data, without taking into account node localization nor node reputation. In [10] an analysis of malicious node behavior during localization is investigated in depth exploiting game of theory concepts, but power consumption and data integrity are not addressed. Thus, DARE extends the results obtained in our previous works defining a hybrid architecture that, in addition to implement secure data aggregation, allows nodes to be localized by using their reputation.

Moreover, an evaluation of the power consumption of DARE architecture and the related battery lifetime is conducted using the energy consumption models presented in [12]. Finally, DARE performances are investigated by means of simulations whose results show that our approach outperforms other solutions. In addition, we developed a prototype to test the practical viability of our approach in realistic settings.

The remaining of the paper is organized as follow: Section 2 summarizes the security model used in this work, while Section 3 describes the DARE network architecture. Section 4 presents the results of the simulation tests, while the results obtained by exploiting a real-world prototype are reported in Section 5. Finally, a brief overview of the state of the art is presented in Section 6; while Section 7 draws some conclusions and provides hints for future works.

2. Security model

The application domains of WSN are really wide spreading from telemedicine to military applications, from ambient monitoring to smart city applications and so on. A lot of such applications provide services that use average data, for example the average temperature, the average pressure. For such a kind of applications it is possible to reduce the amount of data transmitted over the wireless medium using in-network aggregation techniques. Notice that in this case the power consumption of sensor nodes is reduced because sensor nodes use more power during the transmission and reception communication phases than when performing computation [13]. Thus, aggregation protocols may help in reducing the overall traffic among nodes. At the same time, since nodes are the attack goals of malicious users who try to violate the confidentiality and the integrity of data, proper countermeasures are needed to perform a secure data aggregation. Encryption can be used to secure node communication, both hop-by-hop and end-to-end secure data aggregation are supported. In the former case, the data are encrypted by sensing nodes and decrypted by aggregators. The aggregator nodes, then, decrypt the data coming from the sensing nodes, aggregate them, and encrypt them again, until eventually the *Sink* node gets the final encrypted aggregation result (and decrypts it). In the end-to-end approach the intermediate aggregators manipulate only encrypted data and they have no keys to decrypt them. In our work we consider applications that use the aggregated data based on an operation of sum of sensing data. For this kind of data it is possible to use, for example, the additively homomorphic aggregation model define by Castelluccia et al. [4], which allows encrypted data to be aggregated without decrypting the data hop-by-hop. We chose this end-to-end secure aggregation solution in which an attack to any aggregator node is not able to compromise the whole system.

Beside reducing traffic amount in secure manner there is another requirement related to the node position, which requires to be computed by node cooperation (i.e., nodes exchange information in order to allow an estimation). The node positions can be evaluated by using a multilater-